(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 439 497 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.07.2004 Bulletin 2004/30

(51) Int Cl.[7]: **G07B 17/02**

(21) Application number: **03029885.5**

(22) Date of filing: **29.12.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR
Designated Extension States:
AL LT LV MK

(30) Priority: **30.12.2002 US 248248**

(71) Applicant: **PITNEY BOWES INC.**
Stamford, CT 06926-0700 (US)

(72) Inventors:
- **Norris, James, R.**
  Danbury, CT 06810 (US)
- **Rojas, John, W.**
  Norwalk, CT 06855 (US)
- **Coffy, Jean-Hiram**
  Norwalk, CT 06854 (US)
- **Parkos, Arthur**
  Southbury, CT 06488 (US)
- **Leung, Alan**
  New York, NY 10002 (US)
- **Braun, John, F.**
  Fairfield, CT 06824 (US)
- **Leung, Wendy Chui Fen**
  Woodside, NY 11377 (US)

(74) Representative: **HOFFMANN - EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) System and method for authenticating a mailpiece sender

(57) A method and system for authenticating the sender of a mailpiece is described for identifying certain mailpieces as originating from known trusted senders. In one configuration, biometric information and/or biometric metadata is captured when a user writes on a mailpiece with a digital pen (10). That data is then compared to reference data in a database. Registrant data is then loaded into storage device (170) on the mailpiece and may be digitally signed and/or encrypted by the trusted third party. In another configuration, a mailpiece includes the signature of a sender and the biometric data includes authentication data obtained from the signature that is compared to the biometric data related to the signature obtained during a sender registration process.

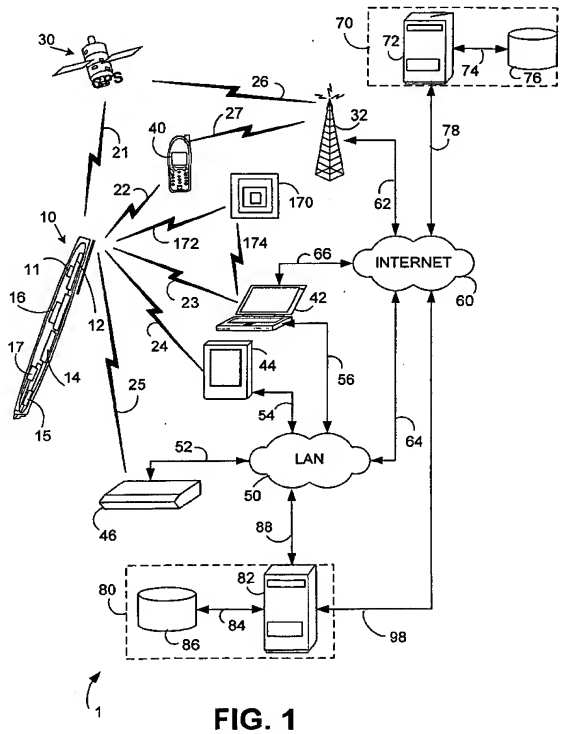


FIG. 1

EP 1 439 497 A2

Description

BACKGROUND

[0001] The illustrative embodiments described in the present application are useful in systems including those for authenticating a sender of an item such as the sender of a mailpiece and more particularly are useful in systems including those for using a digital pen to capture sender biometric data in order to authenticate the sender of a letter.

[0002] The United States Postal Service (USPS) provides a service of mailpiece reception, sorting and delivery to national addresses and international postal streams. The USPS processes approximately 200 billion domestic letters per year. The USPS also processes parcels. Similarly, other courier services provide services for delivery of letters and parcels.

[0003] In 2001, Anthrax spores were found on mail pieces, mail-handling equipment and in or near areas where certain mail pieces that likely contained anthrax spores were handled. These attacks pose a danger of infection that may be lethal to those in the affected areas. Additionally, there is no readily available warning system to provide an early warning that a mail piece contains anthrax spores, other biochemical hazard or other hazardous material. Certain members of the general population may fear receiving and handling mail due to the threat of mail terrorism.

[0004] Previously, the identity of a sender of a mail piece could not be adequately authenticated. Certain mailpieces include postage indicia applied by postage meters that may indicate a postage meter serial number. Mailing machines including postage meters are commercially available from Pitney Bowes Inc. of Stamford, Connecticut.

SUMMARY

[0005] The present application describes several illustrative embodiments of systems and methods for authenticating senders, some of which are summarized here for illustrative purposes. In one illustrative embodiment, a user provides biometric information that is sent to a server. The server then checks this data against a database. If the data matches, the server sends encrypted sender data to the sender that is used by the sender to provide authentication information on the item. In other illustrative embodiments, a user utilizes a digital pen to associate biometric data with a mailpiece. A server authenticates the user by comparing some biometric data to a stored profile and sends authentication data back to the user.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006]

FIG. 1 is a schematic representation of a digital pen system according to an illustrative embodiment of the present application.

FIG. 2A is a schematic representation of an item having authentication storage according to an illustrative embodiment of the present application.

FIG. 2B is a schematic representation of an item having authentication storage according to another illustrative embodiment of the present application.

FIG. 3 is a flow chart showing a process for a user to authenticate the sender of an item according to an illustrative embodiment of the present application.

FIG. 4 is a flow chart showing a process for a server to authenticate the sender of an item according to an illustrative embodiment of the present application.

FIG. 5 is a flow chart showing a process for processing a mailpiece according to an illustrative embodiment of the present application.

DETAILED DESCRIPTION OF EMBODIMENTS

[0007] Systems and methods for authenticating the sender of a item such as a mailpiece are described according to illustrative embodiments of the present application. Previously, the identity of a sender of a mail piece could not be authenticated once the mail piece had been mailed. Accordingly, it was not possible to trust the mailpiece.

[0008] Certain embodiments of the present application describe a method of capturing biometric data such as a person's signature as it is written on an envelope. The signature is then authenticated with a data server over a secure connection to confirm the sender's identity, and then encrypted information about the sender is written to an RF tag (an RFID tag, for example) that is embedded in or on the envelope and that can be later authenticated by a carrier.

[0009] Certain embodiments of the present application authenticate a sender's identity. For the sender who is known as someone who is to be trusted, the mail piece being sent can be assumed to be safe. Therefore, the mail piece does not have to undergo special processing to test for hazardous substances such as Anthrax. While there is no physical test made in order to determine that the mail piece is absolutely safe, it is determined that the sender is known and is considered to be trusted to send safe mail. Once the mail piece has entered the sys-

tem, the data embedded in the RF tag can be used for routing within the postal system.

[0010] In other embodiments, the sender can provide identification to a postal clerk in person at the post office and the mail piece can then be placed in a container used for authenticated mail pieces.

[0011] Digital pens allow a user to capture or digitize handwriting or pen strokes that the user writes on a medium such as a piece of paper. An external processor such as a personal computer may be used. Certain digital pens utilize an imaging device to scan or record an image of the pen stroke. Certain other digital pens use mechanical sensors in order to record a pen stroke. The pen systems may utilize positioning systems such as light-based scanning systems including infrared (ir) sources and detectors in order to determine an absolute or relative position of the pen. Digital pen systems include the N-Scribe system available from Digital Ink of Wellesley, MA and the E-Pen system available from E-Pen InMotion of Matam, Haifa Israel. A digital pointing device includes the V-Pen system available from OTM Technologies of Herzliya Israel.

[0012] Another digital pen system is the Sony-Ericsson CHA-30 Chatpen and Anoto paper available from Anoto AB of Sweden. The Chatpen utilizes a Bluetooth transceiver in order to communicate with a processor. The Anoto paper includes a grid for encoding information such as position information that is detected by the Chatpen. Additional information may be captured including information related to pressure, speed and pen attitude. The additional information includes biometric information that may be used to identify or authenticate a user.

[0013] Commonly owned, Co-pending United States Patent Application Serial No. 10/065,261, entitled Method And System For Creating And Sending A Facsimile Using A Digital Pen, (Attorney Docket No. F-521), filed on September 30, 2002, is incorporated herein by reference in its entirety.

[0014] Commonly owned, co-pending United States Patent Application Serial No. 10/065,282, entitled Method And System For Creating a Document Having Metadata, (Attorney Docket No. F-522), filed on September 30, 2002, is incorporated herein by reference in its entirety.

[0015] Commonly owned, Co-pending United States Patent Application Serial No. 10/065,261, entitled Systems and Methods Using a Digital Pen for Funds Accounting Devices and Postage Meters, (Attorney Docket No. F-575), filed on October 4, 2002, is incorporated herein by reference in its entirety.

[0016] A digital pen is utilized to capture information regarding the pen strokes of a user. In an illustrative embodiment, information regarding the movement of the pen including orientation, pressure, location and time may be captured and analyzed to authenticate a user. In an alternative, other biometric sources such as a retinal scan may be used to authenticate a sender.

[0017] In illustrative embodiments described herein, a system using a Chatpen and Anoto paper is described. However, other digital pen systems may be utilized. Certain digital pens utilize position determination with the actual location of the pen on a piece of paper being used to provide a relative location in terms of the location in the space of the piece of paper. Certain digital pens scan the ink as it is applied in order to digitize a stroke, while yet other pens sense the stroke using sensors such as pressure sensors, Doppler sensors, accelerometers and other sensing mechanisms.

[0018] The Chatpen and Anoto paper system provide for a pen that writes using ink on paper printed with an Anoto pattern. The Chatpen includes a sensor to detect the Anoto pattern. The detected pattern identifies the relative pen location on a grid of the pattern using a pattern look-up processor that may be locally or remotely located. The relative location allows the pen stroke and pattern look-up processor to determine where the pen is on a defined logical space of the pattern. Certain logically defined two-dimensional areas of the pattern may be defined as representing certain functions. For example, Anoto paper may be printed with a box that includes a particular portion of the pattern that is attributed the meaning of Verify Identity process.

[0019] Illustrative embodiments herein describe methods and apparatus for using pen strokes to authenticate a sender. The processes and apparatus described may be implemented using hardware, software or a combination of both. The communications channels may be wireless or wired and may utilize security techniques such as encryption. The data storage and data processors may be locally or remotely located and may use techniques such as load balancing and redundancy.

[0020] Referring to FIG. 1, a first illustrative embodiment describing a sender authentication service system 1 is shown.

[0021] Digital Pen 10 includes a processor 14, memory 12, ink 17, a camera or image sensor 15, a battery 16 and a wireless transceiver 11. It also includes biometric sensors (not shown). In an alternative, the ink 17 is machine detectable. In another embodiment, the ink is invisible. The pen 10 includes a pen tip (not shown) that writes using the ink 17. Writing sensors (not shown) provide data regarding the stroke such as pressure, speed and pen attitude.

[0022] In another alternative, the pen 10 includes audio input/output including synthesized voice output and voice recognition. In an alternative, the pen includes audio indicators such as a speaker, buzzer or speech synthesizer. Visual output is provided using an LCD display and LEDs. Tactile feedback is provided using servomechanisms. Physical input includes an input button.

[0023] The pen 10 includes an rf-id tag writing subsystem (not shown) that is capable of writing to an active or passive rf-id tag 170 adhered to an item using connection 172. The rf-id tag 170 is preferably adhered with semi-permanent glue that can be removed with a sol-

vent. The rf-id tag is a passive tag that uses background rf energy to power the device. Alternatively an active rf-id tag with a power source may be used. The pen 110 can read and write data to the metadata storage device 170. In an alternative, storage tag 170 includes a processor.

[0024] Alternatively, other wireless communication channels can be utilized. In another alternative, a wired communications channel such as a docking station may be utilized in addition to or as a replacement for the wireless transceiver.

[0025] In another alternative, an rf-id tag writer is provided in a co-located processor such as laptop 42 that can write rf-id tag 170 using connection 174. The laptop 42 may be part of a personal area network with the pen 10 and may be used to test that the pen 10 is present in the general location before writing the tag 170. Pen 10 may be docked to laptop 42.

[0026] Using the Chatpen 10, the stroke, biometric and pattern position information is sent to the pen stroke processor via a wireless Bluetooth TM communications channel that is secure across a personal area network. However, a wired connection such as a cradle connected to an IBM compatible PC may be utilized. Bluetooth TM utilizes several layers of security. At a link level, remote/local device authentication is required before any communication can take place. At the Channel level, a link level connection occurs and then the devices need to authenticate before a communications channel is established. Additionally, the data payload being transmitted may be encrypted. In this embodiment, appropriate security at several protocol layers is utilized including the application layer.

[0027] The embodiments described herein may utilize biometric data for purposes including identification and authentication of a user locally as well as to authenticate a user to an authentication server. The pen 10 provides biometric data relating to the pen strokes used including hand speed, pen tip pressure and the inclination angle between pen and paper. Such data is referred to herein as BIODATA. In alternative embodiments, the BIODATA may include other biometric data such as a retinal scan or fingerprint scan performed using an external processor such as laptop 42 that is co-located with the pen or by the pen 10. The pen 10 is assigned a unique identification code that is a unique serial number for the pen. In an alternative, the PUID is a Bluetooth TM MAC code or other unique or group assigned code. In another alternative, the pen user is identified using the BIODATA or other identifier.

[0028] The system 1 includes at least one pen 10 that establishes a personal area network using Bluetooth TM. The paired device may be a Bluetooth TM router 46 that connects to the digital pen 10 using wireless connection 25 and provides a gateway using communications connection 52 to a system LAN 50 or to the Internet 60 (connection not shown). The paired device may include a wireless capable PDA 44 that has a Bluetooth connection 24 and a connection 54 to the LAN 50. Similarly, the digital pen 10 may connect using wireless connection 23 to laptop 42 that is connected to the LAN 50 by connection 56 and the Internet 60 using connection 66. Furthermore, the digital pen 10 may be paired with cellular telephone 40 using connection 22. The cellular telephone 40 is connected to cellular base station 32 using connection 27. Additionally, the digital pen may send or receive signals using satellite 30 using channel 21. The signals may include GPS or other signals. The satellite may be connected to a communications network such as the cellular system using connection 26.

[0029] Here, the system 1 includes an authentication server 80 that includes storage 86 connected by connection 84 to processor 82. The server 80 is connected to the LAN 50 using communications channel 88. Here, the server processes the authentication requests for users. The server 80 is connected to Internet 60 using connection 98 and is connected to carrier system 70.

[0030] In a process described below, a user is authenticated to the authentication server 80 and has at least one biodata profile created using captured biodata such as the recordation of a user signature using a digital pen. In an alternative, any writing sample may be chosen and it does not necessarily have to match the writing that the user will provide when authenticating a mailpiece. Furthermore, server 80 includes an Anoto pattern lookup service for processing Anoto pattern information used by pen 10.

[0031] Carrier system 70 is connected to a network such as the Internet 60 using connection 78. Server 70 includes processor 72 connected to storage 76 using connection 74. Here, the carrier system is preferably the USPS system and includes an rf-id tag reader, information decoder and decryption facilities to enable the rf-id tag data to be read and verified to be authentic.

[0032] The Handheld processor 44 is a PDA including a docking cradle or wireless connection for access to a LAN 50. Coarse position information regarding digital pen 10 location can be determined by locating the paired device such as cellular telephone 40 that can be located by triangulation if transmitting. This data can be sent to server 80 and may be used in the authentication determination (only certain regions are acceptable) and can be sent back to the user with the sender data as an indication of origination.

[0033] Cellular telephone 40 is connected to cellular operator system 32. The cellular telephone could simply provide a data link such as a GSM link. In an alternative, the cellular telephone could include additional processing capacity and be used to capture and/or manipulate data. Corporate LAN 50 is connected to the Internet 60 using T1 line 64. Alternatively, the connections could be over private lines or may be a Virtual Private Network. It is contemplated that all of the connections utilize appropriate security measures.

[0034] Other well-known input devices, servers, processors, networks and communications mechanisms

may be used. A back-end application may be utilized to process pen strokes. The back end application would then recognize command strokes or strokes in command locations identified by the pattern. The data written by a user in a particular data input flied can be rasterized and then subjected to Optical character recognition (OCR) in order to identify the data written by the user.

[0035] Laptop 42 utilizes a mobile Pentium 4 processor and Windows XP. The server processors are geographically and load balanced application servers using systems available from Sun Microsystems and the storage servers use multiple location redundant backup systems. Additionally, other appropriate wireless and wired networks and connections may be utilized. It is contemplated that other communications channels such as OC-3 lines or wireless connections could be used in place of the T1 lines. Similarly, the other communications channels could be replaced with alternatives. Various communication flows may be utilized, some of which will be chattier than others. Laptop 42 could also provide gateway access to the TCP/IP Internet network.

[0036] The present embodiment may alternatively use any pen or stylus like device that provides for electronically recording strokes. Position information may be processed into strokes or transmitted in a separate data stream.

[0037] The digital pen 10 approximates the size of a traditional pen and may be used by a user to handwrite information. The digital pen detects pattern information that may be relayed to a pattern lookup server 70 across the Internet 60. Responsive information may then be sent back to the message processor.

[0038] Here, the co-located processor 44, 42, 40 or remote processor 82 may receive pen data including stroke data, pattern data and other input data. Transmitter/receiver 11 transmits and receives signals to and from the paired base unit 40, 42, 44, 46 that provide a communications link for sending pen data that is used by the back end pen stroke/application layer process to coordinate the authentication process.

[0039] In an alternative, the pen 10 includes the processor for processing pen stroke data and coordinating the authentication process with the authentication server 80. The pen 10 may include a command processor and a communication processor including an analog cellular modem such that the digital pen 10 includes the entire system for requesting an authentication process from server 80. In an alternative, pen 10 and the message processor provide handwriting recognition. The message processor may include handwriting recognition or may employ a limited set of symbol recognition for command processing. Using the Anoto pattern lookup, the system may rely on location in the pattern to determine commands rather than be recognizing strokes.

[0040] In another alternative embodiment, other biometric data may be utilized. For example, the digital pen 10 may be paired with an external processor such as a PDA 50. A shared secret is then provided to the pen 10 and the PDA 50. In one alternative, the user does not type in a device PIN for pairing, but a central data system uses unique identifiers such as MAC codes to pair devices. Thereafter, the PDA could also be used to capture biometric data related to a user. In an alternative, the user is authenticated using a customer number and password. Alternatively, the user could be authenticated using biometrics and the pen could be authenticated using its unique Bluetooth 48 bit MAC address.

[0041] Referring to FIG. 2A, a schematic representation of a representative envelope used for authentication is shown. In an alternative, any item to be sent could be utilized including a label to be placed on a parcel.

[0042] Envelope 200 includes an Anoto pattern area 202. The envelope 200 includes an Anoto pattern sender data area 204. Sender data 204 is utilized to collect biometric data from the user. For example, the user handwrites the user's signature in box 204. The digital pen then collects biometric information including pen movement, orientation, pressure, location and time that can be processed as an authentication packet that is sent to the authentication server for comparison against a profile. A PKI infrastructure can be used to sign and authenticate the packet to a user or to a pen. In an alternative, the user writes a writing sample that is used to collect biometric pen stroke information. The writing sample does not necessarily have to be identical to the sample or samples provided to the authentication server during the account set-up procedure. The user does not have to enter a return address in box 204 because the authentication server is able to lookup that information based upon the biometric data. The server can also store return address information in the storage device 245 such as an rf-id tag. Other storage devices may be used including integrated circuits and 2D bar codes.

[0043] The biometric data may be sent to the authentication server with an ID provided by the digital pen 10 or another processor such as a co-located PDA processor.

[0044] In this illustrative embodiment, the item is an envelope 200. However, the user may instead utilize a label for a parcel or other item. The envelope includes a destination information section 230. The Anoto pattern may be utilized such that the pattern is unique only as to specifying a destination data field. However in an alternative, the Anoto pattern may be unique to the particular user for a controlled envelope in the area of box 204.

[0045] The destination box 230 includes destination address data fields that include the To field 231, an ATTN attention field 232, a first address field ADDR1 133 and a second address field ADDR2 234. The destination box 230 also includes a city field 235, state field 237 and zip field 136.

[0046] The system 1 may be used to recognize the destination address fields 230 using optical character

recognition or other pen stroke recognition methods. In an alternative, only the zip code is processed. In another alternative, the destination address is processed through a known address cleansing process by the authentication server 80 and the cleansed or forwarded address information is stored in rf-id tag 245 without the user knowing that the address was not correct. In an alternative, the user is notified of the potential discrepancy and prompted for a choice among address options.

[0047] Box 210 and identifier 212 are used to notify the local processor that the user has completed entering the challenge information in box 204 and to request authorization. In an alternative, the system waits a predetermined amount of time such as five seconds after the user stops writing in box 204 in order to process the request. Additionally, determining that a user is writing in another box after box 204 can be used as a signal to start the authentication request.

[0048] Additional services may be requested such as a return receipt service by checking in box 214 identified by identifier 216. Similarly, priority mail processing can be requested using check box 222 and identifier 224. In box 218, the user can request the intended recipient be notified of the mailpiece entering the mail stream. The user may also request other track and trace processing. In an alternative, a services box may allow the user to enter service codes that are recognized by analyzing the pen strokes to determine the services requested.

[0049] Referring to FIG. 2B, a schematic representation of a representative envelope used for authentication that has a postage field is shown. Here, a postage value field 290 is used. The user writes a postage amount in the box 290 and the processor recognizes it. The local processor then sends a postage debit request to the authentication server 80 as well as a user authentication request. If the user has the sufficient funds, the amount is debited from the user account and the user is authenticated. In such a manner, postage prepayment is secured before the item is placed in the mail stream. Other data regarding the mailpiece including the services requested and the source and destination addresses may be used to verify the correct postage. The user may be prompted to remedy any under payment.

[0050] Here, the envelope 250 includes Anoto area 252. The Anoto pattern need not be printed on non-data entry areas of the envelope or label.

[0051] Data storage 295 includes a memory such as an rf-id tag or 2D bar code. Address box 280 includes address fields 281, 282, 283, 284, 285, 286 and 287 as above. Service boxes 260, 264, 268 and 172 with respective identifiers 262, 266, 270 and 274 are used as above. User signature area 254 may also be used to enter a writing sample such as "the red fox jumped."

[0052] In an alternative, any item to be sent could be utilized including a label to be placed on a parcel. In another alternative, the envelope 250 could be a reusable envelope in which the Anoto pattern area can be wiped clean for reuse.

[0053] Referring to FIG. 3, a process for initializing a user record and then comparing an authentication data packet to at least one profile is described according to an illustrative embodiment of the present application.

[0054] An envelope is printed with a box 204 for the sender's signature and a check box that is used to initiate the identification and authentication of the sender as illustrated in Figure 2A. The sender signs her name in the Sender's Signature box 204 and then checks the Verify Identity box 210. The pen 10 transmits the signature to the verification system 80 either by wire or wirelessly using a technology such as Bluetooth TM. The verification system looks up the signature in a database containing signatures of persons known to be trusted who have signed up to use the service and have passed appropriate levels of scrutiny to be considered as trusted. Once the signature has been verified, the verification system then writes the sender's name and address and the fact that the signature has been authenticated into the embedded RF tag 245. An authentication certificate may be signed and stored in the tag 245. The verification system 80 can give the sender some type of feedback such as a message box on a CRT or perhaps a beep or a flash of an LED on the pen to indicate that the signature was verified.

[0055] In step 310, the process starts. In step 320, the user obtains a digital pen 10 for use with the service. In step 322, the user registers the device, thereby creating a security profile having biometric data. In one embodiment, the user appears at the office of the authentication server 80 agent to present identification and to provide a writing sample or samples such as a handwritten signature. In an alternative, other biometric information may be collected such as a retinal scan.

[0056] Thereafter, the user account is established and the user may utilize the system to obtain authentication data including authentication indications such as signed codes from the trusted third party authentication server 80. Optionally, the authentication data may include data processed with added services such as address cleansing and may also include sender data and mail processing data such as routing information.

[0057] In step 324, the user obtains an envelope 202 (that may be printed locally by the user) and handwrites the signature in box 204. In step 325, the user request authentication. In step 326, the user receives an authentication notification and the mailpiece is completed. In step 328, the user places the mailpiece in the mail stream and in step 330 the process ends.

[0058] In an alternative, the authentication packet sent to the server 80 may include intended recipient information recognized from the envelope or otherwise available such as data that is electronically available if it is printed on the envelope.

[0059] Referring to FIG 4., a process for providing user authentication data to a user is described according to an illustrative embodiment of the present application. In step 420, the server receives an authentication re-

quest from the client side authentication process that may be located in a digital pen, a coprocessor that is co-located near the digital pen or another processor.

[0060] In step 422, the server receives the biodata. The user request includes a user id and biometric data that will be used in a comparison against a profile. The biodata includes information regarding pen strokes made on an envelope. In an alternative, the biodata is used to determine the user id and the biometric data may be from another source such as a retinal scan.

[0061] In step 424, the authentication server compares the biodata with at least one profile. In step 430, the authentication server determines if the request is valid. If it is not, the process proceeds to step 434 and rejects the request. Remedial action may be taken, such as suspending the account and notifying the relevant carrier of the failure.

[0062] If the request is valid, the authentication server encrypts and signs the authentication data and sends it to the user. The authentication server may also notify the post of the authentication data that may include one or more of routing information, sender information and recipient information. In step 440, the process ends. The trusted third party 80 may digitally sign or encrypt the authentication data send to the user.

[0063] Referring to FIG. 5, a process for accepting items into a carrier system is shown according to an illustrative embodiment of the present application.

[0064] The carrier, such as the postal service, uses RF-ID tag readers in the processing stream to route the mail piece based on the information contained in the tag. For example, the tag may include destination information. If the sender address was authenticated as someone who is known to be trusted, the postal service automatically debits the sender's account for the postage due and routes the mail piece to a processing station for safe mail pieces. In an alternative, the postal service uses several levels of trust based on the individual's credentials. If the sender of a mailpiece is authenticated, but is not known to be trusted, or is at a low level of trust, the mail pieces might be routed to a different processing stage that uses additional inspection techniques to verify the safety of the mail piece. The system can optionally read the recipient's name and address, verify the recipient's address using standard techniques, and then also write that information into the tag for use by the postal service during further routing operations.

[0065] The process 500 starts in step 505. In step 510, the carrier, such as the United States Postal Service (USPS) receives a mailpiece and determines that the mailpiece purports to be from a trusted sender. This determination could be made be sensing the presence of an rf-id tag or other information such as by reading a 2D bar code. The USPS reads the data device on the mailpiece such as the rf-id tag or 2D bar code. The USPS then decodes the information, decrypts the data if it is sent in encrypted form and then authenticates the data. It is preferred that the authentication server 80 provides a signed hash of the authentication data to the user so that that USPS can then authenticate that the information sent by the user to the USPS is actually authenticated as originating at the trusted authentication server system 80.

[0066] In step 515, the USPS determines if the mailpiece was sent by the trusted sender, and if not, the process proceeds to step 535 in which the mailpiece is rejected and any appropriate remedial action initiated.

[0067] In step 520, the mailpiece is authentic. The USPS may then determine whether a post-payment solution is utilized and determine if additional postage is required. Here, as described above, the sender may utilize a traditional payment procedure such as a stamp or meter indicia. Otherwise, in step 525, a postage due amount is calculated and the user account debited. In step 530, the mailpiece is processed as trusted mail. In step 540, the process ends.

[0068] In an alternative, more than one level of trust is utilized and the mailpieces are processed according to the level of trust ranging from complete trust with no secondary procedure, to partial trust with some secondary safe mail procedure and to no trust with a full safe mail decontamination procedure.

[0069] In an alternative, the USPS system 80 also provides the authentication services to the user and a private symmetric key could be used to ensure that an unscrupulous sender did not forge the authentication information.

[0070] In another alternative applicable to any of the embodiments described herein, the user may select a Notify Recipient box shown as shown in FIG 2A. The authentication verification system 80 will perform handwriting recognition on the recipient's name and address that the user has written with the digital pen 10. System 80 will then check its database for an email address entry for the recipient and authorization from the recipient for a notification to be sent. If an email address for the recipient is found, it will be written to the RF tag as authentication data. The postal service will then send an email to the recipient stating that the letter has been mailed by the sender and is in transit. The postal service may also debit the sender's account an additional fee for the notification service. Additional check boxes can be printed on the envelope to be used to select a level of service such as priority mail or for return receipt requests among others.

[0071] In another alternative applicable to any of the embodiments, the RF tag includes tag pre-programming with the sender's name and address when the envelope is purchased. In this alternative, the verification system will know exactly whom the sender is supposed to be based on the information in the tag, and only the sender's signature will be authenticated by the system.

[0072] The privacy of the sender may be protected in several ways. Through the use of an envelope according to an embodiment of the application that does not require sender identity or address, the sender's address

does not need to appear on the envelope. However, if the sender data is not written to the RF tag correctly the postal service would not know where to return the mail piece if needed. The sender's signature or writing sample can also be protected in several ways. The signature verification system does not necessarily use the ink as part of the verification process. Accordingly, in alternative embodiments, the pen could use no ink or use invisible or disappearing ink. Alternatively, the signature box could be placed on the inside flap of the envelope and thus hidden when the envelope is sealed. Finally, the writing sample does not have to be the sender's signature. It can be any written sequence that the system can use for authentication when the postal service signs up the sender as someone who can be trusted.

[0073] In an alternative, the data placed in the RF tag also provides benefits to the postal service by providing for tracking and routing of the mail piece. In certain embodiments, no stamps are required due to the use of the envelope 200 because the RF tag is securely programmed to indicate the amount of postage that has been debited from the sender's account as well as other information that is pertinent.

[0074] In another alternative applicable to any of the embodiments, Wi-Fi enabled wireless systems are utilized and the external processor comprises a Wi-Fi capable hand-held pocket PC such as the Toshiba e740 Pocket PC. Furthermore, differing types of processors and logic systems may be supported. For example, JAVA based PALM OS devices may be utilized. The message logic, processing logic, security logic, user interface logic, communications logic and other logic could be provided in JAVA format or in a format compatible with individual platforms such as Windows CE and PALM OS platform. Similarly, other portable computing devices such as laptop computers and tablet computers and wireless capable computers could be utilized. Other platforms such as those using Symbian OS or OS-9 based portable processors could be utilized.

[0075] In another alternative applicable to any of the embodiments, authentication procedures utilize a token controller having a secure token key storage such as an iButton @ available from Dallas Semiconductor in which an attack, for example, a physical attack on the device, results in an erasure of the key information. Passwords may be used, such as a password to access the device. In an alternative, the password may include biometric data read from a user. Alternatively, other secret key or public key systems may be utilized. Many key exchange mechanisms could be utilized included a Key Encryption Key. Additionally, authentication and repudiation systems such as a secure hash including SHA-1 could be utilized and encryption utilizing a private key for decryption by public key for authentication.

[0076] Known systems such as C++ or Word and VBA may be utilized to implement the processes described. The Anoto toolkits may also be utilized. Authentication data may be used to ensure that only authorized users have access to the rf-id tags. Other systems, processes and postage evidencing methods may be utilized, such as those described in patent applications incorporated by reference above.

[0077] The present application describes illustrative embodiments of a system and method for providing sender authentication. The embodiments are illustrative and not intended to present an exhaustive list of possible configurations. Where alternative elements are described, they are understood to fully describe alternative embodiments without repeating common elements whether or not expressly stated to so relate. Similarly, alternatives described for elements used in more than one embodiment are understood to describe alternative embodiments for each of the described embodiments having that element.

[0078] The described embodiments are illustrative and the above description may indicate to those skilled in the art additional ways in which the principles of this invention may be used without departing from the spirit of the invention. Accordingly, the scope of each of the claims is not to be limited by the particular embodiments described.

Claims

1. A method for providing authorization data for a sender of an item comprising:

   obtaining a digital pen for capturing biometric information;
   registering the digital pen including providing a biometric data sample;
   handwriting a writing sample on the item; and
   sending the item.

2. The method of Claim 1 wherein:

   the item is a label for use with a mailpiece.

3. The method of Claim 1 wherein:

   the item is a mailpiece including an envelope.

4. The method of Claim 1, 2 or 3 wherein:

   the writing sample is a signature.

5. The method of Claim 4 wherein:

   the writing sample is a signature written on the inside of an envelope.

6. The method of any preceding claim further comprising:

   receiving authentication data.

7. The method of Claim 6 further comprising:

storing the authentication data in a storage on an envelope.

8. The method of Claim 7 wherein:

the storage comprises an RF-ID tag.

9. The method of any preceding claim further comprising:

placing the item in the mail stream.

10. The method of any preceding claim further comprising:

receiving an indication that postage was paid.

11. The method of any preceding claim wherein:

the registering process includes providing a writing sample.

12. The method of Claim 11 wherein:

the writing sample comprises a signature.

13. The method of any preceding claim further comprising:

obtaining biometric data relating to the sender.

14. The method of Claim 13 further comprising:

obtaining biometric data relating to the pen strokes of the sender.

15. The method of Claim 13 or 14 further comprising:

creating at least one profile for the sender by analyzing the biometric data.

16. A method for verifying the authenticity of the sender of a mailpiece:

obtaining a mailpiece authentication data from the mail piece;
obtaining a user authentication profile;
comparing a mail piece user profile to the user authentication profile; and
assigning a level of trust to the mailpiece based upon the comparison.

17. The method of Claim 16 wherein:

the user authentication profile include information obtained using user biometric data.

18. The method of Claim 17 wherein:

the user biometric data comprises sample pen stroke data.

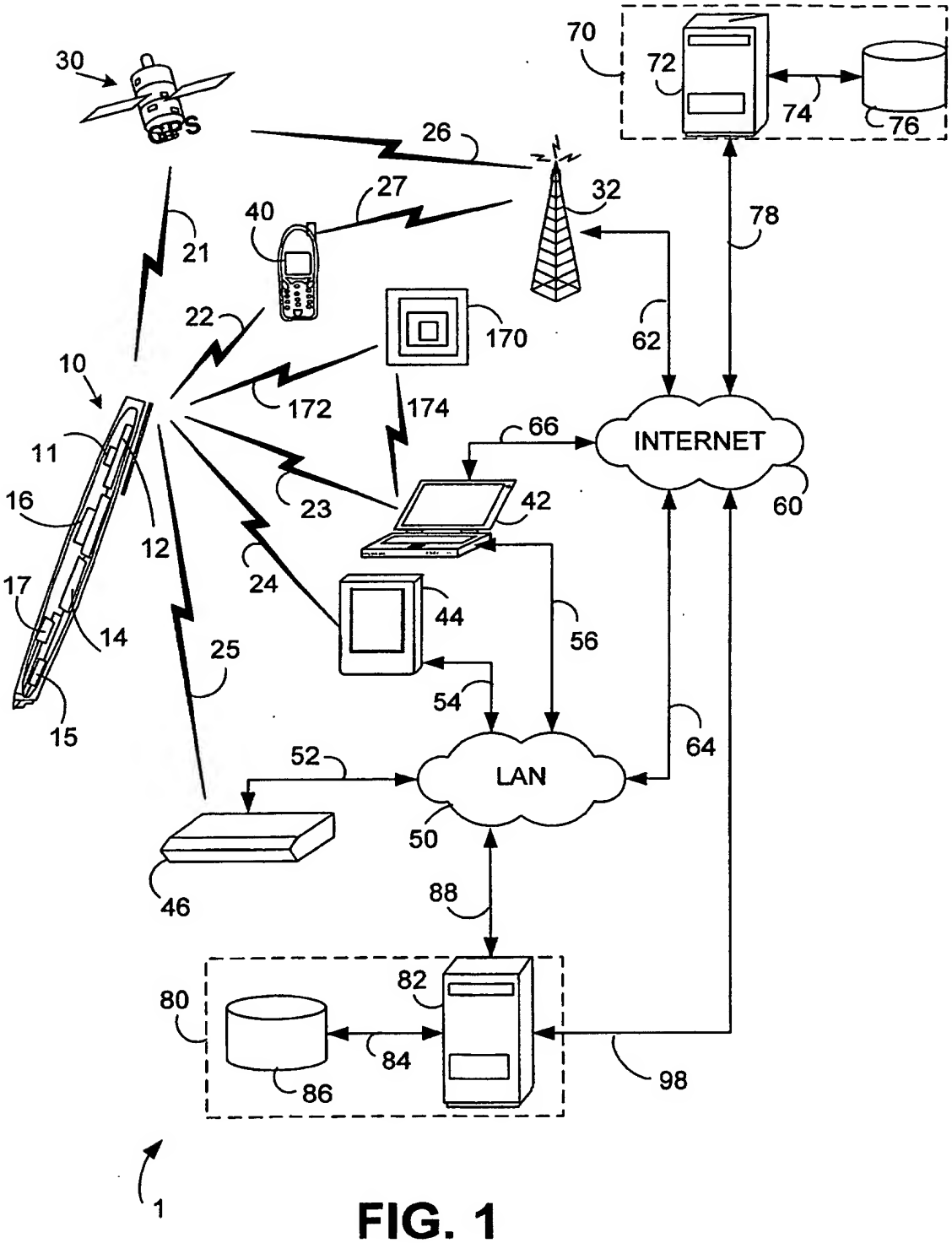

30
GPS
26
70
72
74
76
27
40
32
78
21
22
62
170
10
172
174
66
INTERNET
11
16
23
42
60
12
24
17
44
56
14
25
54
15
52
64
LAN
50
46
88
82
80
84
98
86
1

FIG. 1

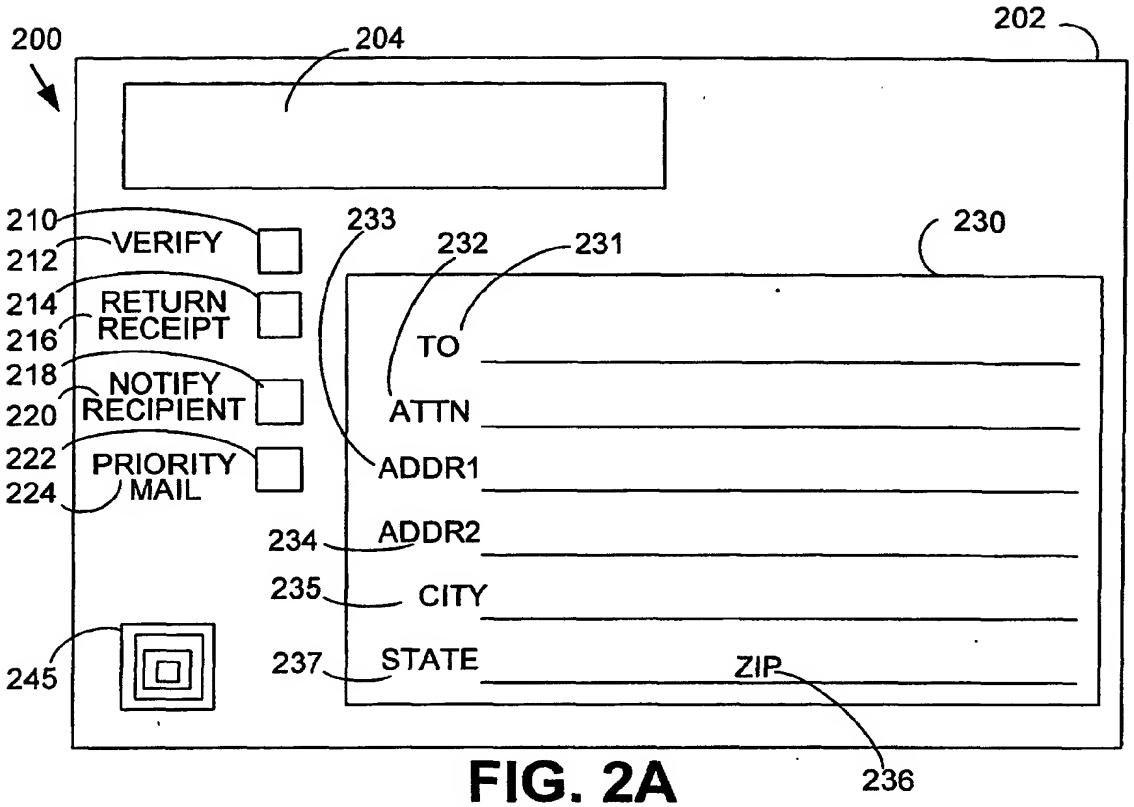

200
202
204
210
VERIFY
212
214
RETURN RECEIPT
216
218
NOTIFY RECIPIENT
220
222
PRIORITY MAIL
224
233
232
231
230
TO
ATTN
ADDR1
234
ADDR2
235
CITY
237
STATE
ZIP
245
236

FIG. 2A

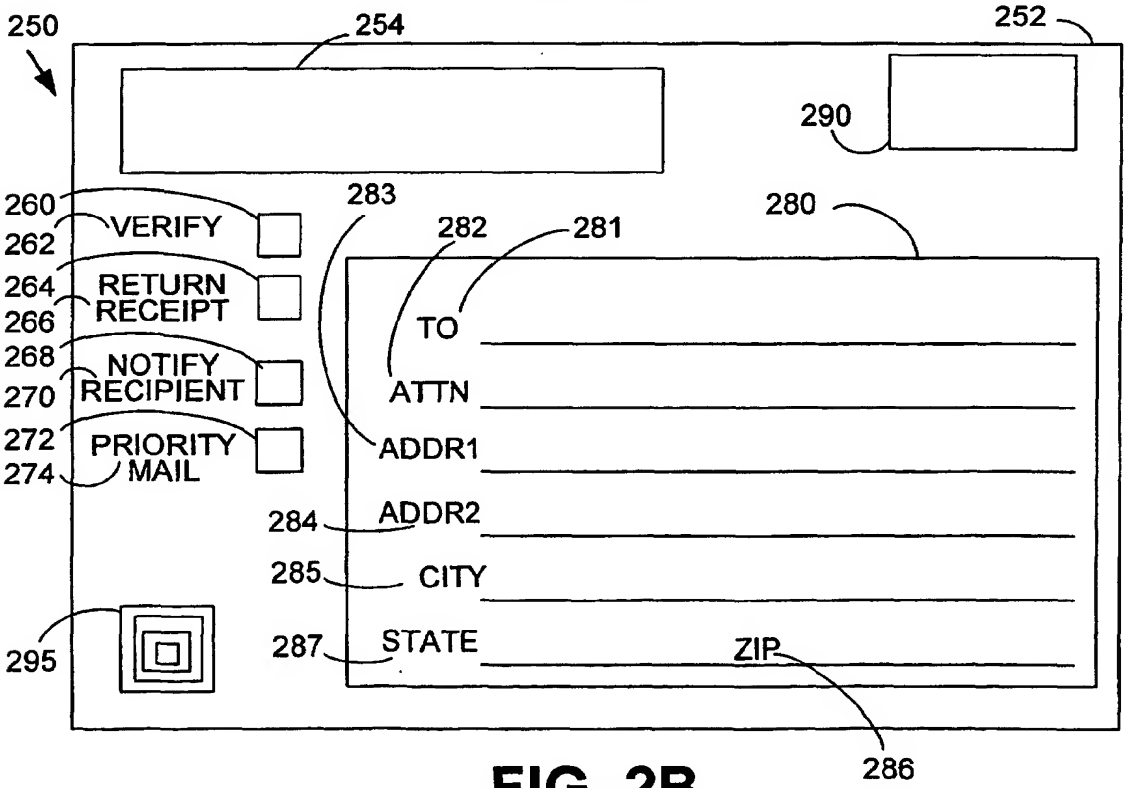

250
252
254
290
260
VERIFY
262
264
RETURN RECEIPT
266
268
NOTIFY RECIPIENT
270
272
PRIORITY MAIL
274
283
282
281
280
TO
ATTN
ADDR1
284
ADDR2
285
CITY
287
STATE
ZIP
295
286

FIG. 2B

FIG. 3

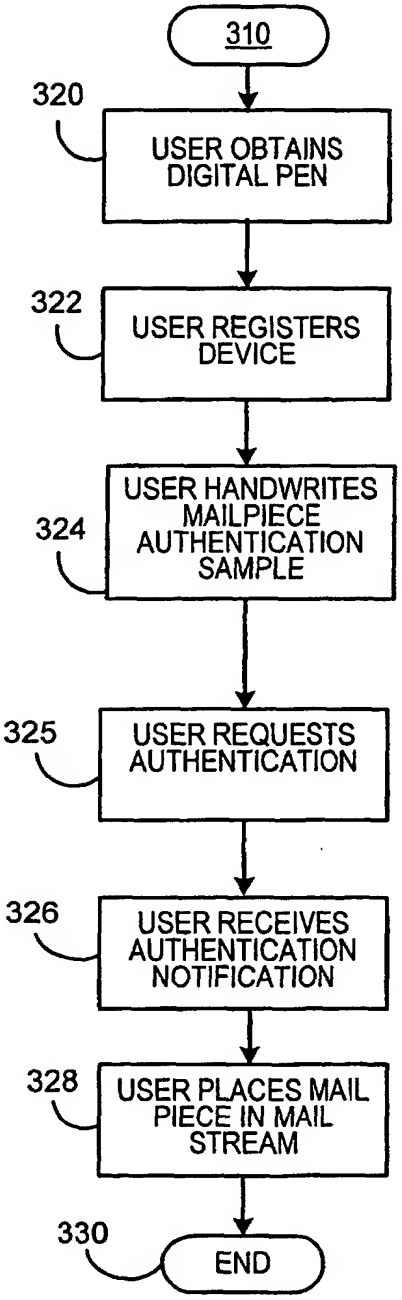
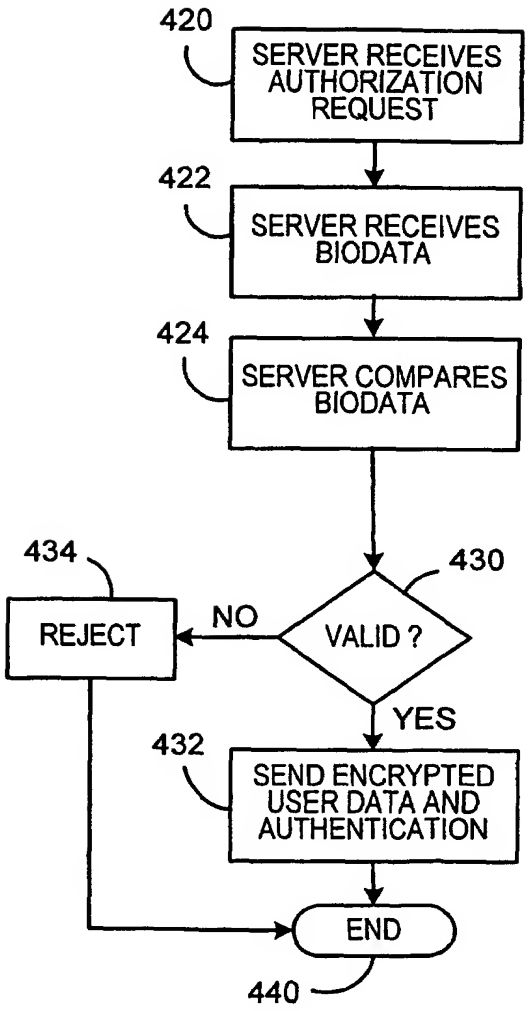

310
320
USER OBTAINS DIGITAL PEN
322
USER REGISTERS DEVICE
USER HANDWRITES MAILPIECE AUTHENTICATION SAMPLE
324
325
USER REQUESTS AUTHENTICATION
326
USER RECEIVES AUTHENTICATION NOTIFICATION
328
USER PLACES MAIL PIECE IN MAIL STREAM
330
END

FIG. 4


420
SERVER RECEIVES AUTHORIZATION REQUEST
422
SERVER RECEIVES BIODATA
424
SERVER COMPARES BIODATA
430
VALID ?
NO
434
REJECT
YES
432
SEND ENCRYPTED USER DATA AND AUTHENTICATION
END
440

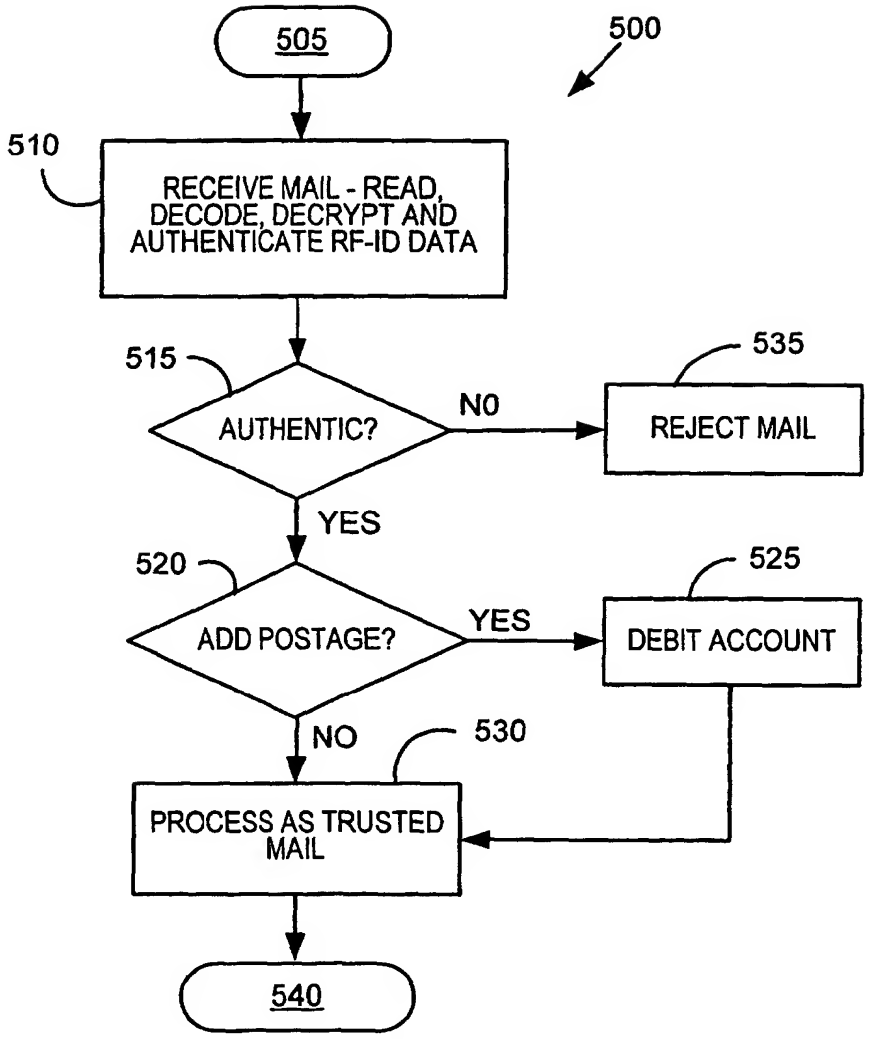

505
500
510
RECEIVE MAIL - READ, DECODE, DECRYPT AND AUTHENTICATE RF-ID DATA
515
AUTHENTIC?
NO
535
REJECT MAIL
YES
520
ADD POSTAGE?
YES
525
DEBIT ACCOUNT
NO
530
PROCESS AS TRUSTED MAIL
540

FIG. 5

PUB-NO: EP001439497A2

DOCUMENT-IDENTIFIER: EP 1439497 A2

TITLE: System and method for authenticating a mailpiece sender

PUBN-DATE: July 21, 2004

INVENTOR-INFORMATION:

NAME	COUNTRY
NORRIS, JAMES R	US
ROJAS, JOHN W	US
COFFY, JEAN-HIRAM	US
PARKOS, ARTHUR	US
LEUNG, ALAN	US
BRAUN, JOHN F	US
LEUNG, WENDY CHUI FEN	US

ASSIGNEE-INFORMATION:

NAME	COUNTRY
PITNEY BOWES	US

APPL-NO: EP03029885

APPL-DATE: December 29, 2003

PRIORITY-DATA: US24824802A (December 30, 2002)

INT-CL (IPC): G07B017/02

EUR-CL (EPC): G07B017/00 , G07B017/00 , G07B017/00

ABSTRACT:

CHG DATE=20060526 STATUS=O>A method and system for authenticating the sender of a mailpiece is described for identifying certain mailpieces as originating from known trusted senders. In one configuration, biometric information and/or biometric metadata is captured when a user writes on a mailpiece with a digital pen (10). That data is then compared to reference data in a database. Registrant data is then loaded into storage device (170) on the mailpiece and may be digitally signed and/or encrypted by the trusted third party. In another configuration, a mailpiece includes the signature of a sender and the biometric data includes authentication data obtained from the signature that is compared to the biometric data related to the signature obtained during a sender registration process.